PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-236662
(43)Date of publication of application : 23.08.2002

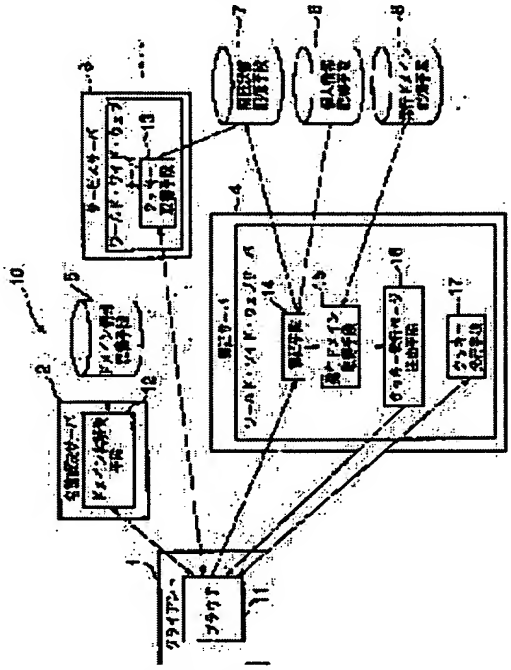
(51)Int.Cl. G06F 15/00

(21)Application number : 2001-031861
(22)Date of filing : 08.02.2001

(71)Applicant : NEC CORP
WEST JAPAN RAILWAY CO
(72)Inventor : JOJIMA TAKAHIRO
KUDO MASATO
YASUFUKU HIROTAKA

(54) INFORMATION PROCESSING SYSTEM AND AUTHENTICATION SERVER PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To receive provision of services on a plurality of service providing servers, which have a plurality of different host names in the Internet respectively, without an Internet browser which has performed log-in once performing the second log-in.
SOLUTION: The server for one log-in is made to have the plurality of host names, and cookies having authentication information for the respective service providing servers are written in the browser by one operation using the server for log-in, thereby inheriting authentication information even in a plurality of domains.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－236662
（P2002－236662A）
(43)公開日　平成14年８月23日(2002.8.23)

(51)Int.Cl.'	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ　５Ｂ０８５

審査請求　未請求　請求項の数12　ＯＬ　（全 11 頁）

(21)出願番号　特願2001－31861(P2001－31861)

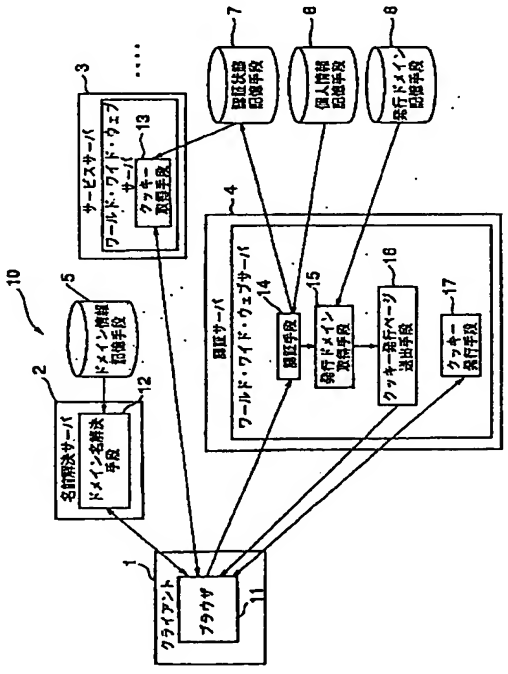
(22)出願日　平成13年２月８日(2001.2.8)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(71)出願人　000196587
西日本旅客鉄道株式会社
大阪府大阪市北区芝田２丁目４番24号
(72)発明者　城島　貴弘
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100071272
弁理士　後藤　洋介　（外１名）

最終頁に続く

(54)【発明の名称】　情報処理システム及び認証サーバプログラム

(57)【要約】
【課題】　インターネットにおける複数の異なるホスト名を持つサービス提供サーバにおいて、一度ログイン処理を行ったインターネット・ブラウザが、再度ログイン処理を行わずに複数のサービス提供サーバ上でサービスの提供を受けることができるようにする。
【解決手段】　一つのログイン処理用のサーバに複数のホスト名を持たせ、そのログイン処理用のサーバで一括して各サービス提供サーバに対する認証情報を持ったクッキーをブラウザに書き込むことにより、複数のドメインにおいても認証情報を引き継げるようにする。



1

【特許請求の範囲】

【請求項１】　クライアントの要求に基づいてクッキーを発行する認証サーバと、前記クッキーが認証されているか判定するサービスサーバとを備え、前記認証サーバは、前記クライアント上で動作するインターネット上の情報を検索し、表示するブラウザからの要求を受信し、前記ブラウザを利用している利用者を個人情報記憶手段に記憶された個人情報から認証し、認証状態記憶手段に認証に関する情報を蓄積する認証手段と、発行ドメイン記憶手段に記憶されている、ブラウザに情報を書き込むためのクッキーを発行するインターネット・ドメイン名を表す発行ドメイン情報を取得し、前記クッキーのドメイン属性を表すドメイン情報を生成する発行ドメイン取得手段と、前記ブラウザに対して前記クッキーを書き込むためのクッキー発行ページを送信するクッキー発行ページ送出手段と、前記ブラウザからの要求に対して前記ブラウザへ前記クッキーの書き込みを行うクッキー発行手段とを備えるとともに、ドメイン名解決手段を用いてインターネット・ドメイン名から通信アドレスへ変換する名前解決サーバを用いて、複数の異なるインターネット・ドメイン名を一つの前記認証サーバの通信アドレスへ関連づけ、複数の前記サービスサーバから共通して認証処理を行えるように構成され、前記サービスサーバは、前記クッキー発行手段で発行された前記クッキーを読み込み、前記ブラウザを利用している前記利用者が認証されているかどうかを判定するクッキー取得手段を備えて構成され、前記認証サーバと前記サービスサーバとが協調して動作することを特徴とする情報処理システム。

【請求項２】　請求項１記載の情報処理システムにおいて、前記認証手段は、前記ブラウザから利用者のＩＤ、パスワードなどの識別情報を受け取り、前記個人情報記憶手段に蓄積されている前記識別情報と比較し、一致するものが前記個人情報記憶手段にあれば新たに利用者に関する認証情報を作成して前記認証状態記憶手段に蓄積し、一致するものがなければ、前記ブラウザに認証失敗を通知することを特徴とする情報処理システム。

【請求項３】　請求項１記載の情報処理システムにおいて、前記発行ドメイン取得手段は、前記発行ドメイン記憶手段から前記発行ドメイン情報を取得し、前記発行ドメイン情報から前記認証サーバを表す文字列を削除したドメイン情報を生成することを特徴とする情報処理システム。

【請求項４】　請求項１記載の情報処理システムにおいて、前記クッキー発行ページ送出手段は、前記認証手段で生成された前記認証情報と、前記発行ドメイン取得手段で取得、生成された前記発行ドメイン情報及び前記ドメイン情報から、前記ブラウザに対して前記クッキーを書き込む前記クッキー発行手段への通信を実行させる前記クッキー発行ページを生成し、ブラウザに返信することを特徴とする情報処理システム。

2

【請求項５】　請求項４記載の情報処理システムにおいて、前記クッキー発行手段は、前記ブラウザで受信した前記クッキー発行ページ中に記述された前記認証情報及び前記ドメイン情報から前記クッキーを生成し、前記ブラウザからの通信要求時に当該クッキーを前記ブラウザに書き込むことを特徴とする情報処理システム。

【請求項６】　請求項１記載の情報処理システムにおいて、前記クッキー取得手段は、インターネット上で利用者に様々なサービスを提供するサービスサーバにおいて、前記クッキー発行手段が前記ブラウザに書き込んだ前記クッキーを読み込み、当該クッキー中に記述された前記認証情報と前記認証状態記憶手段に蓄積された前記認証情報とを比較することにより、前記ブラウザが既に認証されているかどうかを判定することを特徴とする情報処理システム。

【請求項７】　コンピュータに、クライアントの要求に基づいてクッキーを発行する認証サーバの機能をさせるとともに、サービスサーバにおいて前記クッキーが認証されているか判定する機能を備えたサービスサーバプログラムと協調して動作する認証サーバプログラムであって、前記クライアント上で動作するインターネット上の情報を検索し、表示するブラウザからの要求を受信し、前記ブラウザを利用している利用者を個人情報記憶手段に記憶された個人情報から認証し、認証状態記憶手段に認証に関する情報を蓄積する認証手段と、発行ドメイン記憶手段に記憶されている、ブラウザに情報を書き込むためのクッキーを発行するインターネット・ドメイン名を表す発行ドメイン情報を取得し、前記クッキーのドメイン属性を表すドメイン情報を生成する発行ドメイン取得手段と、前記ブラウザに対して前記クッキーを書き込むためのクッキー発行ページを送信するクッキー発行ページ送出手段と、前記ブラウザからの要求に対して前記ブラウザへ前記クッキーの書き込みを行うクッキー発行手段として機能させるとともに、コンピュータにドメイン名解決手段を用いてインターネット・ドメイン名から通信アドレスへ変換する名前解決サーバとして機能させる名前解決サーバプログラムと協調して処理を行い、複数の異なるインターネット・ドメイン名を一つの前記認証サーバの通信アドレスへ関連づけ、複数の前記サービスサーバから共通して認証処理を行うようにコンピュータに機能させることを特徴とする認証サーバプログラム。

【請求項８】　請求項７記載の認証サーバプログラムにおいて、前記認証手段は、前記ブラウザから利用者のＩＤ、パスワードなどの識別情報を受け取り、前記個人情報記憶手段に蓄積されている前記識別情報と比較し、一致するものが前記個人情報記憶手段にあれば新たに利用者に関する認証情報を作成して前記認証状態記憶手段に蓄積し、一致するものがなければ、前記ブラウザに認証

失敗を通知する機能を有すとともに、前記サービスサーバプログラムは、前記クッキー発行手段で発行されたクッキーを読み込み、前記ブラウザを利用している利用者が認証されているかどうかを判定するクッキー取得手段としてコンピュータに機能させるためのプログラムであることを特徴とする認証サーバプログラム。

【請求項９】　請求項７記載の認証サーバプログラムにおいて、前記発行ドメイン取得手段は、前記発行ドメイン記憶手段から前記発行ドメイン情報を取得し、前記発行ドメイン情報から前記認証サーバを表す文字列を削除したドメイン情報を生成することを特徴とする認証サーバプログラム。

【請求項１０】　請求項９記載の認証サーバプログラムにおいて、前記クッキー発行ページ送出手段は、前記認証手段で生成された前記認証情報と、前記発行ドメイン取得手段で取得、生成された前記発行ドメイン情報及び前記ドメイン情報から、前記ブラウザに対して前記クッキーを書き込む前記クッキー発行手段への通信を実行させる前記クッキー発行ページを生成し、ブラウザに返信することを特徴とする認証サーバプログラム。

【請求項１１】　請求項１０記載の認証サーバプログラムにおいて、前記クッキー発行手段は、前記ブラウザで受信した前記クッキー発行ページ中に記述された前記認証情報及び前記ドメイン情報から前記クッキーを生成し、前記ブラウザからの通信要求時に当該クッキーを前記ブラウザに書き込むことを特徴とする認証サーバプログラム。

【請求項１２】　請求項７記載の認証サーバプログラムにおいて、前記クッキー取得手段は、インターネット上で利用者に様々なサービスを提供する前記サービスサーバにおいて機能し、前記クッキー発行手段は前記ブラウザに書き込んだ前記クッキーを読み込み、当該クッキー中に記述された前記認証情報と前記認証状態記憶手段に蓄積された前記認証情報とを比較することにより、前記ブラウザが既に認証されているかどうかを判定する機能を備え、前記サービスサーバと協調することを特徴とする認証サーバプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネットにおけるワールド・ワイド・ウェブ（WWW）に関し、特にワールド・ワイド・ウェブを利用してサーバにアクセスするユーザの認証方法とそのためのプログラムに関する。

【０００２】

【従来の技術】インターネットにおけるワールド・ワイド・ウェブ（WWW）は、ユーザが利用しているクライアントから一般的にインターネットブラウザ（ブラウザ）と呼ばれるプログラムを用いて、ハイパーテキスト転送プロトコル（ＨＴＴＰ）を介してインターネット上

にあるサーバ（WWWサーバ）からファイル及びデータ（リソース）を取得し、ユーザのブラウザ上にテキスト、イメージ、音声などを表示、再生する仕組みである。この時、取得するリソースは、ネットワークを介した接続方法を指定するユニフォーム・リソース・ロケータ（ＵＲＬ）によって指定される。このＵＲＬに関しては、インターネット標準であるＲＦＣ（Ｒｅｆｅｒｅｎｃｅ　Ｆｏｒ　Ｃｏｍｍｅｎｔ）の１７３８番と１８０８番に詳しい。

【０００３】一般に、WWWサーバ上のリソースの取得は、不特定多数のユーザに対して許可されているが、社内文書や個人的な情報のやりとり、金銭の授受などは、サーバに対してログインし、認証を受けた特定ユーザに対してのみ許可する必要がある。この時の認証の方法として、特開平１０－２５７０４８号公報（以下、従来技術１と呼ぶ）で示される方法が挙げられる。この従来技術１による方法では、あるサーバのリソースを取得する際に認証が必要となった時、ユーザが一度サーバにログインすると、サーバはログイン処理により認証されたという旨の情報をユーザが利用するブラウザにクッキー（ｃｏｏｋｉｅ）として書き込む。このクッキーはブラウザの一機能であり、サーバからＨＴＴＰで送信された情報をブラウザ内で記憶でき、以後このブラウザがサーバにアクセスする際にクッキーとしてブラウザ内に蓄積された情報も共に送信させることができる。以後、認証済みのブラウザがサーバにアクセスする際には、サーバ側に認証済みであることを示すクッキーが渡され、サーバは渡されたクッキーで認証情報を取得し、アクセスしてきたブラウザに対して再度ログインさせることなく特定ユーザ向けのリソースを返信する。以上により、ブラウザを利用しているユーザを特定し、一度ログインを行えば再度ログインすることなく、連続して特定ユーザ向けのリソースをサーバから取得することが可能となる。

【０００４】前記クッキーは、“ｈｔｔｐ：／／ｈｏｍｅ．ｎｅｔｓｃａｐｅ．ｃｏｍ／ｎｅｗｓｒｅｆ／ｓｔｄ／ｃｏｏｋｉｅ＿ｓｐｅｃ．ｈｔｍｌ”のＵＲＬで取得できる“ＰＥＲＳＩＳＴＥＮＴ　ＣＬＩＥＮＴ　ＳＴＡＴＥ　ＨＴＴＰ　ＣＯＯＫＩＥＳ”（以下参考文献１と呼ぶ）に詳しい。

【０００５】ここで詳述すると、サーバがブラウザに対してクッキーを書き込む際には、ＨＴＴＰでの通信の際にＳｅｔ－Ｃｏｏｋｉｅヘッダを送信する。Ｓｅｔ－Ｃｏｏｋｉｅヘッダの構文は以下の通りである。

【０００６】Ｓｅｔ－Ｃｏｏｋｉｅ：　ＮＡＭＥ＝ＶＡＬＵＥ；　ｅｘｐｉｒｅｓ＝ＤＡＴＥ；　ｐａｔｈ＝ＰＡＴＨ；　ｄｏｍａｉｎ＝ＤＯＭＡＩＮ＿ＮＡＭＥ；　ｓｅｃｕｒｅ

この構文中、“ＮＡＭＥ＝ＶＡＬＵＥ”の項目は必須の情報であり、他の項目は省略が可能であり、省略した場合は文献１中で示される既定の値が用いられる。以下、

Ｓｅｔ－Ｃｏｏｋｉｅヘッダについて簡略に説明する。“ＮＡＭＥ＝ＶＡＬＵＥ”の項目は、クッキーの名前（ＮＡＭＥ）とその値（ＶＡＬＵＥ）を指定する。“ｅｘｐｉｒｅｓ＝ＤＡＴＥ”の項目は有効期限属性を表し、クッキーの有効期限（ＤＡＴＥ）を指定する。この項目を省略した場合は、ブラウザの終了時点が有効期限となる。“ｄｏｍａｉｎ＝ＤＯＭＡＩＮ＿ＮＡＭＥ”は、ドメイン属性を表し、ブラウザがこのクッキーを送信するサーバのドメイン情報をＤＯＭＡＩＮ＿ＮＡＭＥとして指定する。ドメイン情報の指定は、サーバが持っているインターネット・ドメイン名（以下、ホスト名と呼ぶ）と後方一致で評価が行われる。

【０００７】ホスト名とは、インターネット上でサーバを識別するための名前である。たとえば、“ａｃｍｅ．ｃｏｍ”というドメイン情報をドメイン属性として持つクッキーは、“ａｎｖｉｌ．ａｃｍｅ．ｃｏｍ”や“ｓｈｉｐｐｉｎｇ．ｃｒａｔｅ．ａｃｍｅ．ｃｏｍ”などのホスト名に一致する。ただし、ドメイン属性を持ったクッキーを配布できるサーバは、ドメイン属性で指定したドメイン情報と後方一致するホスト名を持つサーバに限られる。例えば、前記“ａｃｍｅ．ｃｏｍ”というドメイン属性を持つクッキーは、“ｗｗｗ．ｎｅｃ．ｃｏ．ｊｐ”というホスト名とは後方一致しないので、ブラウザは、サーバ“ｗｗｗ．ｎｅｃ．ｃｏ．ｊｐ”からのこのようなクッキーの受け取りを拒否する。この項目を省略した場合は、クッキーを書き込むサーバのホスト名がドメイン情報として利用される。

【０００８】“ｐａｔｈ＝ＰＡＴＨ”の項目は経路属性を表し、ＵＲＬ中で示される経路情報と比較されて、サーバ中のどのリソースを取得する際にクッキーをブラウザが送信すべきかを指定する。“ｓｅｃｕｒｅ”の項目は、この属性が指定されたクッキーは暗号化などで保護されたＨＴＴＰ通信でのみ送信すべきであることを指定する。

【０００９】また、ブラウザがサーバにクッキーを送信する際には、ＨＴＴＰでの通信の際にＣｏｏｋｉｅヘッダを送信する。Ｃｏｏｋｉｅヘッダの構文は以下の通りである。

【００１０】Ｃｏｏｋｉｅ：　ＮＡＭＥ＝ＯＰＡＱＵＥ＿ＳＴＲＩＮＧ；　ＮＡＭＥ＝ＯＰＡＱＵＥ＿ＳＴＲＩＮＧ；　．．．．

各ＮＡＭＥ及びＯＰＡＱＵＥ＿ＳＴＲＩＮＧにＳｅｔ－Ｃｏｏｋｉｅでサーバから書き込まれた“ＮＡＭＥ＝ＶＡＬＵＥ”の各情報が指定される。複数個のクッキーがサーバからブラウザに書き込まれている場合は、“；”で区切られ、複数個並べて送信される。

【００１１】また、特開平１１－２８２８０４号公報（以下、従来技術２と呼ぶ）では、ユーザに対して何らかのサービスをインターネットで提供するためのＷｅｂサービスサーバと、各ユーザを認証するためのＷｅｂ認証サーバとを分離することにより、複数あるＷｅｂサービスサーバでＷｅｂ認証サーバを共有して利用することを可能にしている。これは、ブラウザが通常有しているリダイレクト機能を利用している。Ｗｅｂサービスサーバが提供するリソースにおいてユーザの認証が必要となった場合、Ｗｅｂサービスサーバはブラウザに対してＷｅｂ認証サーバへのリダイレクト命令を送信する。リダイレクト命令を受け取ったブラウザは、リダイレクト命令で指定されたＷｅｂ認証サーバに対してアクセスを行う。ブラウザからアクセスされたＷｅｂ認証サーバは、ブラウザが認証されているかどうかをブラウザに書き込まれているクッキーで判断し、ブラウザが認証されていない場合は、ユーザに対してログインを要求する。ログインが成功した場合には、認証情報をブラウザのクッキーに書き込む。再度認証が起こった場合には、クッキーの認証情報により再びユーザに対してログイン処理を要求することなしに認証済みであることをＷｅｂサービスサーバに通知する。

【００１２】

【発明が解決しようとする課題】前記したように、ブラウザに書き込まれたクッキーがサーバに対して送信される条件は、ドメイン属性で指定したドメイン情報と後方一致するホスト名を持つサーバにアクセスする場合に限定され、かつ；ブラウザにドメイン属性を指定したクッキーを書き込むことが可能なサーバは、ホスト名にドメイン属性で指定したドメイン情報を後方一致の形で含むサーバに限られる。よって、同じドメイン情報をホスト名に含むサーバ同士では同じクッキーの書き込み、取得が可能であるが、違うドメイン名を持つサーバ間では同じクッキーの書き込み、取得ができない。

【００１３】よって、異なるインターネット・ドメイン上で動作しているサイト間で同じ認証情報を用いようとした場合、従来技術ではあるドメイン上のサーバでログインしたユーザの認証情報をブラウザのクッキーとして書き込んだとしても、別のドメイン上のサーバでは当該クッキーを読み込むことができないため認証情報の引き継ぎができない。よって、ユーザは各ドメイン上のサーバを利用する毎にログインをし直し、新たに認証情報を取得する必要がある。

【００１４】そこで、本発明の技術的課題は、インターネットにおける複数の異なるホスト名を持つサービス提供サーバにおいて、一度ログイン処理を行ったインターネット・ブラウザが、再度ログイン処理を行わずに複数のサービス提供サーバ上でサービスの提供を受けることができる情報処理システムとそれに用いられる認証サーバプログラムとを提供することにある。

【００１５】

【課題を解決するための手段】本発明では、一つのログイン処理用のサーバに複数のインターネット・ドメイン名を持たせ、そのログイン処理用のサーバで一括して各

ドメインに対して認証情報を持ったクッキーをブラウザに書き込むことにより、複数のドメインにおいても認証情報を引き継げるようにした情報処理システムを提供するものである。

【００１６】即ち、本発明によれば、クライアントの要求に基づいてクッキーを発行する認証サーバと、前記クッキーが認証されているか判定するサービスサーバとを備え、前記認証サーバは、前記クライアント上で動作するインターネット上の情報を検索し、表示するブラウザからの要求を受信し、前記ブラウザを利用している利用者を個人情報記憶手段に記憶された個人情報から認証し、認証状態記憶手段に認証に関する情報を蓄積する認証手段と、発行ドメイン記憶手段に記憶されている、ブラウザに情報を書き込むためのクッキーを発行するインターネット・ドメイン名を表す発行ドメイン情報を取得し、前記クッキーのドメイン属性を表すドメイン情報を生成する発行ドメイン取得手段と、前記ブラウザに対して前記クッキーを書き込むためのクッキー発行ページを送信するクッキー発行ページ送出手段と、前記ブラウザからの要求に対して前記ブラウザへ前記クッキーの書き込みを行うクッキー発行手段とを備えるとともに、ドメイン名解決手段を用いてインターネット・ドメイン名から通信アドレスへ変換する名前解決サーバを用いて、複数の異なるインターネット・ドメイン名を一つの前記認証サーバの通信アドレスへ関連づけ、複数の前記サービスサーバから共通して認証処理を行えるように構成され、前記サービスサーバは、前記クッキー発行手段で発行された前記クッキーを読み込み、前記ブラウザを利用している前記利用者が認証されているかどうかを判定するクッキー取得手段を備えて構成され、前記認証サーバと前記サービスサーバとが協調して動作することを特徴とする情報処理システムが得られる。

【００１７】また、本発明によれば、前記情報処理システムにおいて、前記認証手段は、前記ブラウザから利用者のＩＤ、パスワードなどの識別情報を受け取り、前記個人情報記憶手段に蓄積されている前記識別情報と比較し、一致するものが前記個人情報記憶手段にあれば新たに利用者に関する認証情報を作成して前記認証状態記憶手段に蓄積し、一致するものがなければ、前記ブラウザに認証失敗を通知することを特徴とする情報処理システムが得られる。

【００１８】また、本発明によれば、前記情報処理システムにおいて、前記発行ドメイン取得手段は、前記発行ドメイン記憶手段から前記発行ドメイン情報を取得し、前記発行ドメイン情報から前記認証サーバを表す文字列を削除したドメイン情報を生成することを特徴とする情報処理システムが得られる。

【００１９】また、本発明によれば、前記情報処理システムにおいて、前記クッキー発行ページ送出手段は、前記認証手段で生成された前記認証情報と、前記発行ドメイン取得手段で取得、生成された前記発行ドメイン情報及び前記ドメイン情報から、前記ブラウザに対して前記クッキーを書き込む前記クッキー発行手段への通信を実行させる前記クッキー発行ページを生成し、ブラウザに返信することを特徴とする情報処理システムが得られる。

【００２０】また、本発明によれば、前記情報処理システムにおいて、前記クッキー発行手段は、前記ブラウザで受信した前記クッキー発行ページ中に記述された前記認証情報及び前記ドメイン情報から前記クッキーを生成し、前記ブラウザからの通信要求時に当該クッキーを前記ブラウザに書き込むことを特徴とする情報処理システムが得られる。

【００２１】また、本発明によれば、前記情報処理システムにおいて、前記クッキー取得手段は、インターネット上で利用者に様々なサービスを提供するサービスサーバにおいて、前記クッキー発行手段が前記ブラウザに書き込んだ前記クッキーを読み込み、当該クッキー中に記述された前記認証情報と前記認証状態記憶手段に蓄積された前記認証情報とを比較することにより、前記ブラウザが既に認証されているかどうかを判定することを特徴とする情報処理システムが得られる。

【００２２】また、本発明によれば、コンピュータに、クライアントの要求に基づいてクッキーを発行する認証サーバの機能をさせるとともに、サービスサーバにおいて前記クッキーが認証されているか判定する機能を備えたサービスサーバプログラムと協調して動作する認証サーバプログラムであって、前記クライアント上で動作するインターネット上の情報を検索し、表示するブラウザからの要求を受信し、前記ブラウザを利用している利用者を個人情報記憶手段に記憶された個人情報から認証し、認証状態記憶手段に認証に関する情報を蓄積する認証手段と、発行ドメイン記憶手段に記憶されている、ブラウザに情報を書き込むためのクッキーを発行するインターネット・ドメイン名を表す発行ドメイン情報を取得し、前記クッキーのドメイン属性を表すドメイン情報を生成する発行ドメイン取得手段と、前記ブラウザに対して前記クッキーを書き込むためのクッキー発行ページを送信するクッキー発行ページ送出手段と、前記ブラウザからの要求に対して前記ブラウザへ前記クッキーの書き込みを行うクッキー発行手段として機能させるとともに、コンピュータにドメイン名解決手段を用いてインターネット・ドメイン名から通信アドレスへ変換する名前解決サーバとして機能させる名前解決サーバプログラムと協調して処理を行い、複数の異なるインターネット・ドメイン名を一つの前記認証サーバの通信アドレスへ関連づけ、複数の前記サービスサーバから共通して認証処理を行うようにコンピュータに機能させることを特徴とする認証サーバプログラムが得られる。

【００２３】また、本発明によれば、前記認証サーバプ

ログラムにおいて、前記認証手段は、前記ブラウザから利用者のＩＤ、パスワードなどの識別情報を受け取り、前記個人情報記憶手段に蓄積されている前記識別情報と比較し、一致するものが前記個人情報記憶手段にあれば新たに利用者に関する認証情報を作成して前記認証状態記憶手段に蓄積し、一致するものがなければ、前記ブラウザに認証失敗を通知する機能を有するとともに、前記サービスサーバプログラムは、前記クッキー発行手段で発行されたクッキーを読み込み、前記ブラウザを利用している利用者が認証されているかどうかを判定するクッキー取得手段としてコンピュータに機能させるためのプログラムであることを特徴とする認証サーバプログラムが得られる。

【００２４】また、本発明によれば、前記認証サーバプログラムにおいて、前記発行ドメイン取得手段は、前記発行ドメイン記憶手段から前記発行ドメイン情報を取得し、前記発行ドメイン情報から前記認証サーバを表す文字列を削除したドメイン情報を生成することを特徴とする認証サーバプログラムが得られる。

【００２５】また、本発明によれば、前記認証サーバプログラムにおいて、前記クッキー発行ページ送出手段は、前記認証手段で生成された前記認証情報と、前記発行ドメイン取得手段で取得、生成された前記発行ドメイン情報及び前記ドメイン情報から、前記ブラウザに対して前記クッキーを書き込む前記クッキー発行手段への通信を実行させる前記クッキー発行ページを生成し、ブラウザに返信することを特徴とする認証サーバプログラムが得られる。

【００２６】また、本発明によれば、前記認証サーバプログラムにおいて、前記クッキー発行手段は、前記ブラウザで受信した前記クッキー発行ページ中に記述された前記認証情報及び前記ドメイン情報から前記クッキーを生成し、前記ブラウザからの通信要求時に当該クッキーを前記ブラウザに書き込むことを特徴とする認証サーバプログラムが得られる。

【００２７】また、本発明によれば、前記認証サーバプログラムにおいて、前記クッキー取得手段は、インターネット上で利用者に様々なサービスを提供する前記サービスサーバにおいて機能し、前記クッキー発行手段は前記ブラウザに書き込んだ前記クッキーを読み込み、当該クッキー中に記述された前記認証情報と前記認証状態記憶手段に蓄積された前記認証情報とを比較することにより、前記ブラウザが既に認証されているかどうかを判定する機能を備え、前記サービスサーバと協調することを特徴とする認証サーバプログラムが得られる。

【００２８】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照しながら説明する。

【００２９】図１は本発明の実施の形態による情報処理システムの構成を示す図である。

【００３０】図１に示すように、情報処理システム１０では、一般ユーザが利用する不特定多数のクライアント１と、インターネット上の名前から実際の通信アドレスに変換するための名前解決サーバ２と、実際にインターネットを通してユーザにサービスを提供するためのワールド・ワイド・ウェブ・サーバ（ＷＷＷサーバ）が動作している複数のサービスサーバ３と、ユーザのログイン処理を行って認証を行う認証サーバ４とを備えて構成される。ここで、クライアント１と名前解決サーバ２、サービスサーバ３、及び認証サーバ４とは、インターネットなどのネットワークを介して接続されている。名前解決サーバ２、サービスサーバ３、及び認証サーバ４の各機能は、名前解決サーバプログラム、サービスサーバプログラム、及び認証サーバプログラム４によって、コンピュータに夫々行わせることができる。

【００３１】クライアント１上には、ブラウザ１１が動作しており、名前解決サーバ２やサービスサーバ３、認証サーバ４と通信を行い、サーバ上のリソースの取得を行う。

【００３２】また、名前解決サーバ２上にはドメイン名解決手段１２が動作しており、ドメイン情報記憶手段１５１に記憶された情報を元にインターネット上のホストを示したホスト名から実際の通信アドレスへの変換処理を行っている。ドメイン名解決手段１２は一般にドメイン・ネーム・サーバ（ＤＮＳ）と呼ばれるものであり、インターネットの標準を記述したＲＦＣの１０３４番と１０３５番とに規定されている。

【００３３】表１はドメイン情報記録手段５の内容例を示している。

【００３４】

【表１】

インターネット上のホスト名	通信アドレス
www.jr-odekake.net	123.4.5.6
www.jrwest.co.jp	10.5.6.7

【００３５】表１に示す例では、「ｗｗｗ．ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔ」というホスト名が「１２３．４．５．６」という通信アドレスに変換され、「ｗｗｗ．ｊｒｗｅｓｔ．ｃｏ．ｊｐ」というホスト名は「１０．５．６．７」という通信アドレスに変換されることを示している。

【００３６】ドメイン名解決手段１２は、複数の名前解決サーバ２上で協調して動作していてもよく、また、ドメイン情報記憶手段５も複数あって構わない。

【００３７】サービスサーバ３にはＷＷＷサーバが動作しており、ブラウザ１１からのＨＴＴＰを利用した通信を受け取り、リソースを返信する。このＷＷＷサーバはサーバの機能拡張機構があり、当該機構を利用して、ブラウザ１１にクッキーとして蓄積された認証情報を取得

するためのクッキー取得手段１３が動作している。

【００３８】また、認証サーバ４上にもサービスサーバ３と同じもしくは同機能を持つＷＷＷサーバが動作しており、ブラウザ１１からのＨＴＴＰを利用した通信を受け取り、ログイン処理を行う。このＷＷＷサーバは、サーバの機能拡張機構があり、その機構を利用してブラウザ１１からのログイン要求を受け取り実際のログイン処理を行う認証手段１４、ログインが成功した場合にクッキーを発行するドメイン情報を取得する発行ドメイン取得手段１５、発行ドメイン取得手段１５で取得したドメイン情報に基づいてブラウザ１１に対しクッキーを書き込むためのクッキー発行ページを送出するためのクッキー発行ページ送出手段１６、実際にブラウザ１１に対してクッキーを発行するためのクッキー発行手段１７が動作している。また、ブラウザ１１を利用しているユーザの個人情報を蓄積するための個人情報記憶手段６とブラウザ１１の認証状態を蓄積するための認証状態記憶手段７とクッキーを発行する認証サーバ４のホスト名を蓄積するための発行ドメイン記憶手段８とがサービスサーバ３及び認証サーバ４に接続されている。

【００３９】個人情報記憶手段６、認証状態記憶手段７、発行ドメイン記憶手段８は、システム構築の手間を軽減するため、ワールド・ワイド・ウェブサーバ内に実装しても構わない。

【００４０】本発明の実施の形態の具体例として、３つのサービスサーバ３が存在し、そのホスト名が「ｗｗｗ．ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔ」、「ｗｗｗ．ｎｅｃ．ｃｏ．ｊｐ」、「ｅｃｓｉｔｅ．ｊｒｗｅｓｔ．ｃｏ．ｊｐ」の名前を持っていたとする。この時、それぞれのサービスサーバ３のドメイン情報は、「ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔ」、「ｎｅｃ．ｃｏ．ｊｐ」、「ｊｒｗｅｓｔ．ｃｏ．ｊｐ」とする。

【００４１】本発明の実施の形態における認証サーバ４は、それぞれのサーバ用のドメイン情報に認証サーバ４であることを示す文字列を付加して、複数のホスト名を持つ。例えば認証サーバ４であることを示す文字列を「ｎｉｎｓｙｏｕ」とすると、「ｎｉｎｓｙｏｕ．ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔ」、「ｎｉｎｓｙｏｕ．ｎｅｃ．ｃｏ．ｊｐ」、「ｎｉｎｓｙｏｕ．ｊｒｗｅｓｔ．ｃｏ．ｊｐ」の３つの名前を持つ。ここで認証サーバ４が持つホスト名は、共通して認証を行うサービスサーバ３のドメイン情報の種類の数だけホスト名を持つ。ある複数のサービスサーバ３が同じドメイン情報を持つ場合には、認証サーバ４はそのドメイン情報に対して一つのホスト名を持つだけでよい。

【００４２】下記表２は、この時のドメイン情報記憶手段の例を示している。

【００４３】

【表２】

インターネット上のホスト名	通信アドレス
www.jr-odekake.net	123.4.5.6
ninsyou.jr-odekake.net	123.4.5.100
www.nec.co.jp	192.168.1.10
ninsyou.nec.co.jp	123.4.5.100
ecsite.jrwest.co.jp	10.5.6.8
ninsyou.jrwest.co.jp	123.4.5.100

【００４４】上記表２に示すように、各サービスサーバが、「ｗｗｗ．ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔ」、「ｗｗｗ．ｎｅｃ．ｃｏ．ｊｐ」、「ｅｃｓｉｔｅ．ｊｒｗｅｓｔ．ｃｏ．ｊｐ」として登録されており、それぞれの通信アドレスが「１２３．４．５．６」、「１９２．１６８．１．１０」、「１０．５．６．８」と設定されている。また認証サーバ４の各サービスサーバ３に対応するホスト名が、「ｎｉｎｓｙｏｕ．ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔ」、「ｎｉｎｓｙｏｕ．ｎｅｃ．ｃｏ．ｊｐ」、「ｎｉｎｓｙｏｕ．ｊｒｗｅｓｔ．ｃｏ．ｊｐ」として登録されており、各ホスト名は同じ認証サーバ４を指すので通信アドレスは同一のものとなる。ここでドメイン情報記憶手段５に記憶されている認証サーバ４を示す通信アドレスが異なっていた場合、通信の経路を制御する一般にルータ及びスイッチと呼ばれる通信アドレスの変換機能を持つ機器を利用して最終的に同一の通信アドレスを示すようにしても構わない。また、認証サーバ４が複数の通信機器を装備し、複数の通信アドレスを利用できる場合は、ドメイン情報記憶手段５で記憶されている認証サーバ４を示す通信アドレスは複数の通信アドレスで示されても構わない。

【００４５】表３はこの時の発行ドメイン記憶手段８の持つドメイン情報を示している。

【００４６】

【表３】

発行ドメイン情報
ninsyou.jr-odekake.net
ninsyou.nec.co.jp
ninsyou.jrwest.co.jp

【００４７】図２はユーザのログイン処理についての動作を示すフローチャート図である。

【００４８】図２を参照しながら、以上の例を元に、ユーザのログイン処理について説明する。

【００４９】まず、認証サーバ４は、ＷＷＷサーバ上の認証手段１４でブラウザ１１を利用しているユーザのＩＤとパスワードをブラウザ１１から受け取る（ステップＳ１）。この時、指紋情報などのユーザを特定できる情報であるならば、ＩＤとパスワードの代わりとして利用してもよい。ＩＤとパスワードを受け取った認証手段１

４は、個人情報記憶手段６に蓄積されているＩＤ及びパスワードとブラウザ１１から受け取ったＩＤとパスワードとを比較する（ステップＳ２）。

【００５０】表４は、この時の個人情報記憶手段６の一例を示している。

【００５１】

【表４】

ID	パスワード
XYZ00001	QLsiJD11
…	…

【００５２】上記表４に示すように、この例では、ＩＤ「ＸＹＺ００００１」のユーザのパスワードは「ＱＬｓｉＪＤ１１」であることを示す。個人情報記憶手段６では、前記ＩＤとパスワードの他にもユーザに関する氏名や住所などの情報も併せて記憶していてもよい。また、ＩＤ、パスワードなどの情報は何らかの暗号方法で暗号化されていてもよい。次に、ＩＤ及びパスワードの比較の結果、一致するかどうかを確認し（ステップＳ３）、一致しなかった場合ブラウザ１１に対して認証失敗を通知して（ステップＳ４）ログイン処理を終了する。一致した場合には、ブラウザ１１が認証済みであることを示す認証情報を生成する（ステップＳ５）。この認証情報は、ブラウザ１１毎に固有な値となればどのような値でもかまわない。生成された認証情報は、認証状態記憶手段７にＩＤと共に蓄積される（ステップＳ６）。

【００５３】表５はこの時の認証状態記憶手段７の一例を示している。

【００５４】

【表５】

ID	認証情報
XYZ00001	IOJ99312-3333jd
…	…

【００５５】表５に示す例では、ＩＤ「ＸＹＺ００００１」が認証情報「ＩＯＪ９９３１２－３３３３ｊｄ」で認証されていることを示す。この時、認証情報記憶手段７では、前記ＩＤと認証情報の他にログイン成功時の時間なども蓄積して、時間切れ処理などに利用してもかまわない。次に、発行ドメイン取得手段１５は、発行ドメイン記憶手段８からクッキーの発行ドメイン情報を取得する（ステップＳ７）。

【００５６】表３の例では、「ｎｉｎｓｙｏｕ．ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔ」、「ｎｉｎｓｙｏｕ．ｎｅｃ．ｃｏ．ｊｐ」、「ｎｉｎｓｙｏｕ．ｊｒｗｅｓｔ．ｃｏ．ｊｐ」が取得される。発行ドメイン取得手段１５は、取得した発行ドメイン情報から認証サーバ４を示す文字列を削除した、ドメイン情報を作成する（ステップＳ８）。前記の例では、「ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔ」、「ｎｅｃ．ｃｏ．ｊｐ」、「ｊｒｗｅｓｔ．ｃｏ．ｊｐ」が作成される。次に、クッキー発行ページ送出手段１６は、ステップＳ５、Ｓ７、及びＳ８で生成、取得された認証情報、発行ドメイン情報、ドメイン情報を元にクッキー発行ページを作成し、ブラウザ１１に返信する（ステップＳ９）。

【００５７】図３は前記例におけるクッキー発行ページの例を示す図である。図３に示すように、このクッキー発行ページは、一般にＨＴＭＬと呼ばれる記述言語で記述され、ブラウザ１１で解釈されることによりブラウザ１１に対して様々な処理を命令することができる。ＨＴＭＬに関しては、“ｈｔｔｐ：／／ｗｗｗ．ｗ３ｃ．ｏｒｇ／ＭａｒｋＵｐ／”のＵＲＬで取得できる“ＨｙｐｅｒＴｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ　Ｈｏｍｅ　Ｐａｇｅ”に詳しい。

【００５８】図３で示されるＨＴＭＬ記述のうち、クッキー発行に関する記述は＜ＦＲＡＭＥ　．．．．＞で示される行である。＜ＦＲＡＭＥ　．．．　＞は、ＳＲＣの項目で示されるＵＲＬにアクセスすることをブラウザ１１１に命令する。例えば、＜ＦＲＡＭＥ　ＳＲＣ＝“ｈｔｔｐ：／／ｎｉｎｓｙｏｕ．ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔ／ｃｏｏｋｉｅ？Ｃ＿ＩＤ＝ＩＯＪ９９３１２－３３３３ｊｄ＆ＤＯＭ＿ＮＡＭＥ＝ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔ”＞は、ｎｉｎｓｙｏｕ．ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔで示される認証サーバ４から、ｃｏｏｋｉｅという名前で指定されるクッキー発行手段１７に対して、認証情報「ＩＯＪ９９３１２－３３３３ｊｄ」をＣ＿ＩＤとして、クッキーのドメイン情報「ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔ」をＤＯＭ＿ＮＡＭＥとして引数に指定し、アクセスすることをブラウザ１１に命令している。この時、ブラウザ１１が＜ＦＲＡＭＥ　．．．＞記述を処理できない場合に備えて、＜ＮＯＦＲＡＭＥＳ＞記述を用い、＜ＦＲＡＭＥ．．．＞記述の代わりに＜ＩＭＡＧＥ　．．．＞記述を用いても構わない。また、クッキー発行ページに記述する＜ＦＲＡＭＥ　．．．＞は一つだけにしておき、クッキー発行手段１７の返信中に他のホスト名でアクセスされるクッキー発行手段１７を呼び出す記述を行い、順々にクッキーを発行するようにしてもよい。クッキー発行ページを受け取ったブラウザ１１は、ページ内のＨＴＭＬ記述に従い認証サーバ４上のクッキー発行手段１７にアクセスする（ステップＳ１０）。クッキー発行手段１７は、アクセス時のＵＲＬ中にＣ＿ＩＤとして記述された認証情報をクッキーの値として指定し、ＤＯＭ＿ＮＡＭＥとして指定されたドメイン情報をドメイン属性としてクッキー情報を作成し、ブラウザ１１へ前記したＨＴＴＰのＳｅｔ－Ｃｏｏｋｉｅヘッダを利用して書き込む（ステップＳ１１）。例えば、クッキー発行手段１７が＜ＦＲＡＭＥ　ＳＲＣ＝“ｈｔｔｐ：／／ｎｉｎｓｙｏｕ．ｊｒ－ｏｄｅｋａｋ

ｅ．ｎｅｔ／ｃｏｏｋｉｅ？Ｃ＿ＩＤ＝ＩＯＪ９９３１２－３３３３ｊｄ＆ＤＯＭ＿ＮＡＭＥ＝ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔ”＞のＨＴＭＬ記述で呼び出された場合、認証情報が「ＩＯＪ９９３１２－３３３３ｊｄ」、ドメイン情報が「ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔ」となり、クッキー発行手段１７は、「Ｓｅｔ－Ｃｏｏｋｉｅ：　Ｃ＿ＩＤ＝ＩＯＪ９９３１２－３３３３ｊｄ；ｄｏｍａｉｎ＝ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔ」というヘッダをブラウザ１１に対して送信する。このヘッダを受け取ったブラウザ１１は前記したように、クッキー発行手段１７が「ｈｔｔｐ：／／ｎｉｎｓｙｏｕ．ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔ」のホスト名で参照されており、クッキーに指定されたドメイン属性「ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔ」を含んでいることからクッキーの書き込みを許可し、名前が「Ｃ＿ＩＤ」で値が「ＩＯＪ９９３１２－３３３３ｊｄ」のクッキーを保存する。ブラウザ１１は、クッキー発行ページ中に記述されている＜ＦＲＡＭＥ＞記述の分だけ、ステップＳ１０、ステップＳ１１を繰り返す。

【００５９】例では、ｎｉｎｓｙｏｕ．ｊｒ－ｏｄｅｋａｋｅ．ｎｅｔ、ｎｉｎｓｙｏｕ．ｎｅｃ．ｃｏ．ｊｐ、ｎｉｎｓｙｏｕ．ｊｒｗｅｓｔ．ｃｏ．ｊｐ上のクッキー発行手段１７を参照することになるが、これは表２に示されている通り、すべて同じ認証サーバ４に対する通信アドレスを示している。

【００６０】以上のＳ１～Ｓ１１のステップにより、ログインに成功したブラウザ１１上には、ローカル・エリア・ネットワーク上にある各サービスサーバ３用のクッキーが書き込まれる。

【００６１】次に、図４は特定ユーザ向けのサービスを提供しているサービスサーバ３が、ブラウザ１１からのアクセスを受けた場合の認証処理の説明に供せられる図である。図４を参照すると、まず、サービスサーバ３は、ブラウザ１１からアクセスがあった場合に、ブラウザ１１が認証情報をクッキーとして送信しているかを調べる（ステップＳ２１）。この時、ブラウザ１１が前述したステップＳ１～Ｓ１１のステップによりログイン処理を行っているならば、前記したようにブラウザ１１は認証サーバ４へのＨＴＴＰ通信中にＣｏｏｋｉｅヘッダを付加し、このＣｏｏｋｉｅヘッダでクッキーとして記憶した認証情報を認証サーバ４へ送信する。

【００６２】もし、ブラウザ１１が認証情報をクッキーとして送信していなければ認証サーバ４では認証情報を受信できず、そのブラウザ１１は認証されていないとして特定ユーザ向けのサービスを拒否する（ステップＳ２２）。認証サーバ４で認証情報をクッキーとして受信できれば、当該認証情報が認証状態記憶手段７で蓄積されているかどうかを調べる（ステップＳ２３，Ｓ２４）。この時、安全性を高めるため暗号技術などを用いて当該認証情報が正しいかどうかを確認する処理を行ってもよい。受信した認証情報が認証記憶手段７で蓄積されていなければ、不正な認証情報であるとして特定ユーザ向けのサービスを拒否する（Ｓ２５）。受信した認証情報が認証記憶手段７に蓄積されていれば、アクセスしてきたブラウザ１１は既に認証済みであるとし、特定ユーザ向けのサービスの利用をブラウザ１１に許可する。ステップＳ２１～Ｓ２６の各ステップにより、各サービスサーバ３はアクセスしてきたブラウザ１１が認証済みであるかどうかを判別できる。なお、ステップＳ２２、Ｓ２５の各ステップにおいて特定ユーザ向けのサービスを拒否した場合、転送などの処理を行いユーザに対して認証サーバ４でのログイン処理を促してもよい。

【００６３】以上、ステップＳ１～Ｓ１１、Ｓ２１～Ｓ２６の各ステップにおけるクライアント１及びサービスサーバ３、認証サーバ４間の通信には、安全性を高めるため、通信内容の暗号化を行うのが望ましい。また、サービスサーバ３、認証サーバ４、個人情報記憶手段６、認証状態記憶手段７、発行ドメイン記憶手段８とは、安全性を高めるため同一ローカル・エリア・ネットワーク上で動作させる方が望ましい。また、ブラウザ１１との通信の際には、一般にファイアー・ウォールとして知られている通信装置を使用して、通信の安全性を高める方が望ましい。

【００６４】

【発明の効果】以上説明したように、本発明を利用することにより、ブラウザを利用しているユーザは、ただ一度ログインすればドメインの異なる複数のサービスサーバで認証情報が共有されるため、各サーバ毎にログインをやり直す手間がなくなり、これにより、あるサービスサーバを利用しているユーザを他のドメイン上で動作しているサービスサーバへ誘導することが容易となり、サービスを利用するユーザ数を増加させることができる情報処理システムを提供することができる。

【００６５】また、本発明においては、各サービスサーバを構築する際には、どのようなインターネット・ドメイン名を名乗ってもよく、サービスの内容に即したユーザの覚えやすいインターネット・ドメイン名を使用でき、これにより、サービスサーバのインターネット・ドメイン名を不特定多数のユーザに深く印象づけることが可能となり、サービスを利用するユーザ数を増加させることができる情報処理システムを提供することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態による情報処理システムを示すブロック図である。

【図２】図１の情報処理システムの動作説明に供せられるフローチャート図である。

【図３】本発明の実施の形態の情報処理システムにより発行されたクッキー発行ページの一例を示す図である。

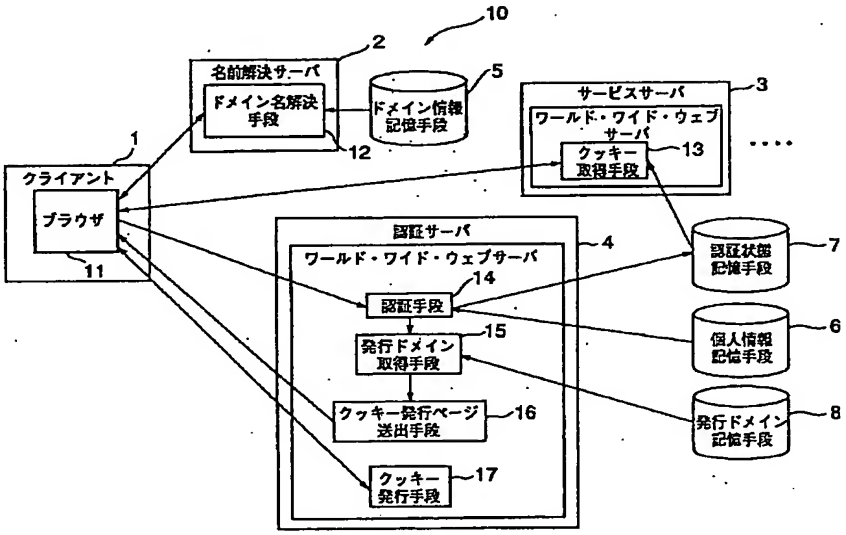
【図４】本発明の実施の形態による情報処理システムの

サービスサーバにおける認証済みブラウザの判定処理を示すフローチャート図である。

【符号の説明】

1　クライアント
2　名前解決サーバ
3　サービスサーバ
4　認証サーバ
5　ドメイン情報記憶手段
6　個人情報記憶手段
7　認証状態記憶手段
＊8　発行ドメイン記憶手段
10　情報処理システム
11　ブラウザ
12　ドメイン名解決手段
13　クッキー取得手段
14　認証手段
15　発行ドメイン取得手段
16　クッキー発行ページ送出手段
17　クッキー発行手段
＊10

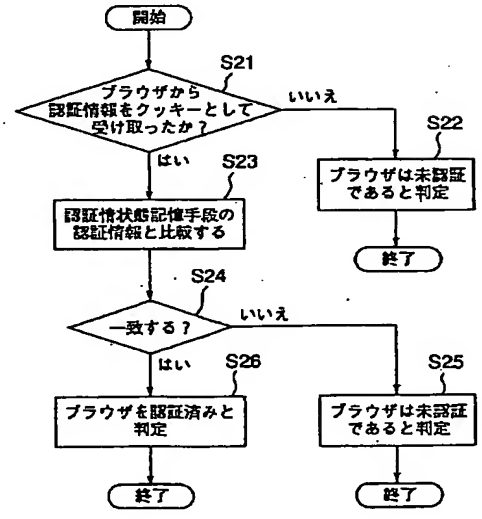
【図１】



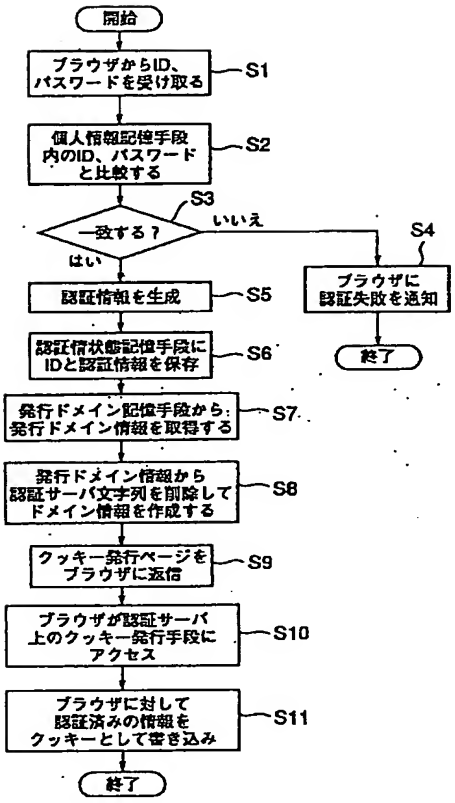
【図３】

```
<HTML><HEAD>ログイン完了</TITLE></HEAD>
<FRAMESET ROWS="0,*">
<FRAME SRC="http://ninsyou.jr-odekake.net/cookie?C_ID=
IOJ99312-3333jd&DOM_NAME=jr-odekake.net">
<FRAME SRC="http://ninsyou.nec.co.jp/cookie?C_ID=
IOJ99312-3333jd&DOM_NAME=nec.co.jp">
<FRAME SRC="http://ninsyou.jrwest.co.jp/cookie?C_ID=
IOJ99312-3333jd&DOM_NAME=jrwest.co.jp">
<FRAMESET></HTML>
```

【図４】



【図２】



フロントページの続き

(72)発明者　工藤　正人
東京都港区芝五丁目７番１号　日本電気株式会社内

(72)発明者　安福　弘貴
大阪府大阪市北区芝田二丁目４番24号　西日本旅客鉄道株式会社内

Ｆターム(参考)　5B085 AE02 AE23 BG07

* NOTICES *

JPO and NCIPI are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

Bibliography

---

(19) [Publication country] Japan Patent Office (JP)
(12) [Kind of official gazette] Open patent official report (A)
(11) [Publication No.] JP,2002-236662,A (P2002-236662A)
(43) [Date of Publication] August 23, Heisei 14 (2002. 8.23)
(54) [Title of the Invention] Information processing system and an authentication server program
(51) [The 7th edition of International Patent Classification]

G06F 15/00 330

[FI]

G06F 15/00 330 B

[Request for Examination] Un-asking.
[The number of claims] 12
[Mode of Application] OL
[Number of Pages] 11
(21) [Application number] Application for patent 2001-31861 (P2001-31861)
(22) [Filing date] February 8, Heisei 13 (2001. 2.8)
(71) [Applicant]
[Identification Number] 000004237
[Name] Nippon Electric Co., Ltd.
[Address] 5-7-1, Shiba, Minato-ku, Tokyo
(71) [Applicant]
[Identification Number] 000196587
[Name] West Japan Railway Co.
[Address] 2-4-24, Shibata, Kita-ku, Osaka-shi, Osaka
(72) [Inventor(s)]
[Name] Jojima Takahiro
[Address] 5-7-1, Shiba, Minato-ku, Tokyo Inside of Nippon Electric Co., Ltd.
(72) [Inventor(s)]
[Name] Kudo Forward people
[Address] 5-7-1, Shiba, Minato-ku, Tokyo Inside of Nippon Electric Co., Ltd.
(72) [Inventor(s)]
[Name] Yasufuku Hirotaka
[Address] 2-4-24, Shibata, Kita-ku, Osaka-shi, Osaka A West Japan Railway stock meeting in the company
(74) [Attorney]
[Identification Number] 100071272
[Patent Attorney]
[Name] Goto Yosuke (besides one person)
[Theme code (reference)]

5B085

[F term (reference)]

5B085 AE02 AE23 BG07

[Translation done.]

* NOTICES *

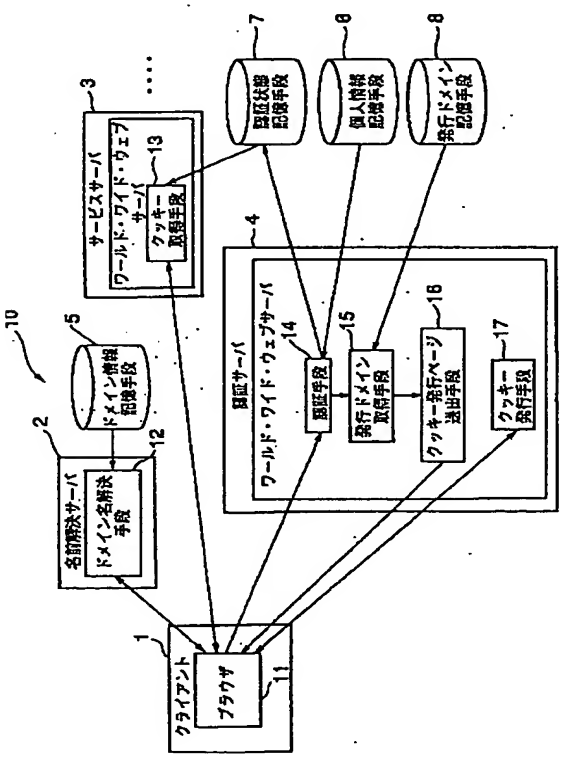
JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

Epitome

(57) [Abstract]
[Technical problem] The Internet browser which performed log in processing once enables it to receive offer of service on two or more service provision servers in a service provision server with the host name from which the plurality in the Internet differs, without performing log in processing again.
[Means for Solution] It enables it to succeed authentication information also in two or more domains by writing in a browser the Cookie which gave two or more host names to one server for log in processing, bundled up by the server for the log in processing, and had the authentication information over each service provision server.

[Translation done.]



[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any

damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The name resolution server both changed into the communication link address from the Internet domain name using a domain name solution means as it is characterized by providing the following is used. The Internet domain name from which plurality differs is related with the communication link address of said one authentication server. It is constituted so that authentication processing can be performed in common from said two or more service servers. Said service server Read said Cookie published with said Cookie issuance means, and have a Cookie acquisition means to judge whether said user using said browser is attested, and it is constituted. Information processing system characterized by said authentication server and said service server operating in cooperation The authentication server which publishes Cookie based on the demand of a client It is an authentication means is equipped with whether said Cookie is attested and the service server to judge, and said authentication server retrieves the information on the Internet which operates on said client, and receives the demand from the browser to display, attests the user using said browser from the individual humanity news memorized by the individual humanity news storage means, and accumulate the information about authentication in an authentication condition storage means. An issuance domain acquisition means to generate the domain information which acquires the issuance domain information that the Internet domain name which publishes Cookie for writing information in a browser memorized by the issuance domain storage means is expressed, and expresses the domain attribute of said Cookie A Cookie issuance page sending-out means to transmit the Cookie issuance page for writing in said Cookie to said browser, and the Cookie issuance means which writes in said Cookie to said browser to the demand from said browser
[Claim 2] In information processing system according to claim 1 said authentication means Identification information, such as a user's ID and a password, from said browser Reception, If the authentication information about a user will newly be created and it will accumulate in said authentication condition storage means as compared with said identification information accumulated in said individual humanity news storage means, if a match is in said individual humanity news storage means, and there is no match Information processing system characterized by notifying authentication failure to said browser.
[Claim 3] It is the information processing system characterized by generating the domain information which deleted the character string which said issuance domain acquisition means acquires said issuance domain information from said issuance domain storage means in information processing system according to claim 1, and expresses said authentication server from said issuance domain information.
[Claim 4] It is the information processing system characterized by to generate said Cookie issuance page which performs the communication link to said Cookie issuance means which writes in said Cookie to said browser from said authentication information by which said Cookie issuance page sending-out means was generated with said authentication means in information processing system according to claim 1, and said issuance domain information acquired and generated with said issuance domain acquisition means and said domain information, and to answer a browser.
[Claim 5] It is the information processing system characterized by generating said Cookie from said authentication information described in said Cookie issuance page which received said Cookie issuance means by said browser in information processing system according to claim 4, and said domain information, and writing the Cookie concerned in a communication link demand from said browser at said browser.
[Claim 6] In information processing system according to claim 1 said Cookie acquisition means In the service server which provides a user with various services on the Internet By reading said Cookie which said Cookie issuance means wrote in said browser, and comparing said authentication information described in the Cookie concerned with said authentication information accumulated in said authentication condition storage means Information processing system characterized by judging whether said browser is already attested.
[Claim 7] While carrying out the function of the authentication server which publishes Cookie to a computer based on the demand of a client It is the authentication server program which operates in harmony with the service server program equipped with whether said Cookie is attested in the service server, and the function to judge. Retrieve the information on the Internet which operates on said client, and the demand from the browser

to display is received. An authentication means to attest the user using said browser from the individual humanity news memorized by the individual humanity news storage means, and to accumulate the information about authentication in an authentication condition storage means, The issuance domain information that the Internet domain name which publishes Cookie for writing information in a browser memorized by the issuance domain storage means is expressed is acquired. An issuance domain acquisition means to generate the domain information showing the domain attribute of said Cookie, A Cookie issuance page sending-out means to transmit the Cookie issuance page for writing in said Cookie to said browser, While making it function as a Cookie issuance means which writes in said Cookie to said browser to the demand from said browser It processes in harmony with the name resolution server program operated as a name resolution server which uses a domain name solution means for a computer, and is changed into the communication link address from the Internet domain name. The authentication server program characterized by making it function on a computer as relating with the communication link address of said one authentication server the Internet domain name from which plurality differs, and performing authentication processing in common from said two or more service servers.
[Claim 8] In an authentication server program according to claim 7 said authentication means Identification information, such as a user's ID and a password, from said browser Reception, If the authentication information about a user will newly be created and it will accumulate in said authentication condition storage means as compared with said identification information accumulated in said individual humanity news storage means, if a match is in said individual humanity news storage means, and there is no match While having the function which notifies authentication failure to said browser, said service server program The authentication server program characterized by being a program for operating as a computer whether the user who read the Cookie published with said Cookie issuance means, and uses said browser is attested as a Cookie acquisition means to judge.
[Claim 9] It is the authentication server program characterized by generating the domain information which deleted the character string which said issuance domain acquisition means acquires said issuance domain information from said issuance domain storage means in an authentication server program according to claim 7, and expresses said authentication server from said issuance domain information.
[Claim 10] It is the authentication server program characterized by for said Cookie issuance page sending-out means to generate said Cookie issuance page which performs the communication link to said Cookie issuance means which writes in said Cookie to said browser from said authentication information generated with said authentication means, and said issuance domain information acquired and generated with said issuance domain acquisition means and said domain information in an authentication server program according to claim 9, and to answer a browser.
[Claim 11] It is the authentication server program characterized by generating said Cookie from said authentication information described in said Cookie issuance page which received said Cookie issuance means by said browser in the authentication server program according to claim 10, and said domain information, and writing the Cookie concerned in a communication link demand from said browser at said browser.
[Claim 12] In an authentication server program according to claim 7 said Cookie acquisition means In said service server which provides a user with various services, it functions on the Internet. Said Cookie issuance means by reading said Cookie written in said browser, and comparing said authentication information described in the Cookie concerned with said authentication information accumulated in said authentication condition storage means The authentication server program characterized by having the function to judge whether said browser is already attested, and cooperating with said service server.

[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to authentication approach and program of a sake of the user who accesses a server especially using World Wide Web about the World Wide Web (WWW) in the Internet.
[0002]
[Description of the Prior Art] The World Wide Web (WWW) in the Internet is structure which acquires a file and data (resource) from the server (WWW server) which is generally on the Internet through a HyperText Transfer Protocol (HTTP) using the Internet browser (browser) and a called program from the client which the user uses, displays a text, an image, voice, etc. and is reproduced on a user's browser. The resource to acquire is specified by the uniform resource locator (URL) which specifies the connection method through a network at this time. It is detailed to No. 1738 of RFC (Reference For Comment) which is the Internet criterion about this URL, and No. 1808.
[0003] Generally, although acquisition of the resource on a WWW server is permitted to many and unspecified users, the exchange of an in-house document or individual information, transfer of money, etc. need to log in to a server, and need to permit authentication only to a carrier beam specification user. As the approach of the authentication at this time, the approach shown by JP,10-257048,A (it is hereafter called the conventional technique 1) is mentioned. By the approach by this conventional technique 1, when acquiring the resource of a certain server and authentication is needed, once a user logs in to a server, a server will be written in the browser for which a user uses the information on the purport that it was attested by log in processing as Cookie (cookie). This Cookie is one function of a browser, can memorize within a browser the information transmitted by HTTP from the server, and in case this browser accesses a server henceforth, it can also make both the information accumulated into the browser as Cookie transmit. Henceforth, in case a browser [finishing / authentication] accesses a server, the Cookie in which it is shown that it is authentication ending is passed to a server side, and a server answers a letter in the resource for specific users, without acquiring authentication information and making it log in again to the accessed browser with the passed Cookie. It becomes possible to acquire the resource for specific users from a server continuously by the above, without logging in again, once it specifies the user using a browser and logs in.
[0004] Said Cookie is detailed to "PERSISTENT CLIENT STATE HTTP COOKIES" (it is called reference 1 below) acquirable by URL of "http: / /home.netscape.com/newsref/std/cookie_spec.html."
[0005] If it explains in full detail here, in case a server will write in Cookie to a browser, a Set-Cookie header is transmitted in the case of the communication link by HTTP. The functor of a Set-Cookie header is as follows.
[0006] Set-Cookie: NAME=VALUE; expires=DATE; path=PATH; domain=DOMAIN_NAME; secure — the item of "NAME=VALUE" is indispensable information among this functor, other items are omissible, and when it omits, the fixed value shown in reference 1 is used. Hereafter, a Set-Cookie header is explained simple. The item of "NAME=VALUE" specifies the identifier (NAME) and value of Cookie (VALUE). The item of "expires=DATE" expresses an expiration date attribute and specifies the expiration date (DATE) of Cookie. When this item is omitted, the termination event of a browser serves as an expiration date. "domain=DOMAIN_NAME" expresses a domain attribute and specifies as DOMAIN_NAME the domain information on a server that a browser transmits this Cookie. Assessment is performed by the Internet domain name (it is hereafter called the host name) and right side match in which the server has assignment of domain information.
[0007] A host name is an identifier for identifying a server on the Internet. For example, the Cookie which has the domain information of "acme.com" as a domain attribute is in agreement with host names, such as "anvil.acme.com" and "shipping.crate.acme.com." However, the server which can distribute Cookie with a domain attribute is restricted to a server with the host name which carries out a right side match to the domain information specified with the domain attribute. For example, since the right side match of the Cookie with the domain attribute of the above "acme.com" is not carried out to the host name "www.nec.co.jp", a browser refuses the reception of such Cookie from a server "www.nec.co.jp." When this item is omitted, the host name of the server which writes in Cookie is used as domain information.
[0008] In case the item of "path=PATH" expresses a path attribute, is compared with the path information shown in URL and which resource in a server is acquired, it specifies whether a browser should transmit Cookie. It specifies that the Cookie with which, as for the item of "secure", this attribute was specified should be transmitted only by the HTTP communication link protected by encryption etc.
[0009] Moreover, in case a browser transmits Cookie to a server, a Cookie header is transmitted in the case of the communication link by HTTP. The functor of a Cookie header is as follows.
[0010] Cookie: NAME=OPAQUE_STRING; NAME=OPAQUE_STRING; ....
Each information on "NAME=VALUE" written in each NAME and OPAQUE_STRING from the server by Set-Cookie is specified. When two or more Cookie is written in the browser from the server, it is divided by";", and

more than one are put in order and it is transmitted.
[0011] Moreover, in JP,11-282804,A (it is hereafter called the conventional technique 2), it makes it possible to share and use a Web authentication server by the Web Service server which has more than one by separating the Web Service server for offering a certain service by the Internet to a user, and the Web authentication server for attesting each user. This uses the redirection function which the browser usually has. When a user's authentication is needed in the resource which a Web Service server offers, a Web Service server transmits the redirection instruction to a Web authentication server to a browser. The browser which received the redirection instruction is accessed to the Web authentication server specified with a redirection instruction. The Web authentication server accessed from the browser requires a log in of a user, when it judges whether the browser is attested or not with the Cookie in which it is written by the browser and the browser is not attested. When a log in is successful, authentication information is written in the Cookie of a browser. When authentication takes place again, it notifies that it is authentication ending to a Web Service server, without requiring log in processing of a user again using the authentication information on Cookie.
[0012]
[Problem(s) to be Solved by the Invention] The server which can write in the Cookie which the conditions to which the Cookie written in the browser is transmitted to a server as described above were limited when a server with the host name which carries out a right side match to the domain information specified with the domain attribute was accessed, and specified the domain attribute as the browser is restricted to the server which includes the domain information specified as the host name with the domain attribute in the form of a right side match. Therefore, although the writing of the same Cookie and acquisition are possible at the servers which include the same domain information in a host name, the writing of the same Cookie and acquisition cannot be performed between servers with a different domain name.
[0013] Therefore, in the server on another domain, though the authentication information of the user who logged in by the server on the domain which is the conventional technique is written in as Cookie of a browser when it is going to use the same authentication information between the sites which are operating on a different Internet domain, since the Cookie concerned cannot be read, taking over of authentication information cannot be performed. Therefore, whenever a user uses the server on each domain, he needs to do a log in again, and he newly needs to acquire authentication information.
[0014] Then, the technical technical problem of this invention has the Internet browser which performed log in processing once in a service provision server with the host name from which the plurality in the Internet differs in offering the information processing system which can receive offer of service on two or more service provision servers, without performing log in processing again, and the authentication server program used for it.
[0015]
[Means for Solving the Problem] In this invention, the information processing system which enabled it to succeed authentication information also in two or more domains is offered by writing in a browser the Cookie which gave two or more Internet domain names to one server for log in processing, bundled up by the server for the log in processing, and had authentication information to each domain.
[0016] According to this invention, it has the authentication server which publishes Cookie based on the demand of a client, and whether said Cookie is attested and the service server to judge. Namely, said authentication server Retrieve the information on the Internet which operates on said client, and the demand from the browser to display is received. An authentication means to attest the user using said browser from the individual humanity news memorized by the individual humanity news storage means, and to accumulate the information about authentication in an authentication condition storage means, The issuance domain information that the Internet domain name which publishes Cookie for writing information in a browser memorized by the issuance domain storage means is expressed is acquired. An issuance domain acquisition means to generate the domain information showing the domain attribute of said Cookie, A Cookie issuance page sending-out means to transmit the Cookie issuance page for writing in said Cookie to said browser, While having the Cookie issuance means which writes in said Cookie to said browser to the demand from said browser The name resolution server changed into the communication link address from the Internet domain name using a domain name solution means is used. The Internet domain name from which plurality differs is related with the communication link address of said one authentication server. It is constituted so that authentication processing can be performed in common from said two or more service servers. Said service server Read said Cookie published with said Cookie issuance means, and have a Cookie acquisition means to judge whether said user using said browser is attested, and it is constituted. The information processing system characterized by said authentication server and said service server operating in cooperation is obtained.
[0017] According to this invention, it sets to said information processing system. Moreover, said authentication means Identification information, such as a user's ID and a password, from said browser Reception, If the

authentication information about a user will newly be created and it will accumulate in said authentication condition storage means as compared with said identification information accumulated in said individual humanity news storage means, if a match is in said individual humanity news storage means, and there is no match The information processing system characterized by notifying authentication failure to said browser is obtained.
[0018] Moreover, according to this invention, in said information processing system, said issuance domain acquisition means acquires said issuance domain information from said issuance domain storage means, and the information processing system characterized by generating the domain information which deleted the character string showing said authentication server from said issuance domain information is obtained.
[0019] According to this invention, it sets to said information processing system. Moreover, said Cookie issuance page sending-out means It acquires with said authentication information generated with said authentication means, and said issuance domain acquisition means. Said Cookie issuance page which performs the communication link to said Cookie issuance means which writes in said Cookie to said browser from said generated issuance domain information and said domain information is generated, and the information processing system characterized by answering a browser is obtained.
[0020] Moreover, according to this invention, in said information processing system, said Cookie issuance means generates said Cookie from said authentication information described in said Cookie issuance page received by said browser, and said domain information, and the information processing system characterized by writing the Cookie concerned in a communication link demand from said browser at said browser is obtained.
[0021] According to this invention, it sets to said information processing system. Moreover, said Cookie acquisition means In the service server which provides a user with various services on the Internet By reading said Cookie which said Cookie issuance means wrote in said browser, and comparing said authentication information described in the Cookie concerned with said authentication information accumulated in said authentication condition storage means The information processing system characterized by judging whether said browser is already attested is obtained.
[0022] Moreover, while carrying out the function of the authentication server which publishes Cookie to a computer based on the demand of a client according to this invention It is the authentication server program which operates in harmony with the service server program equipped with whether said Cookie is attested in the service server, and the function to judge. Retrieve the information on the Internet which operates on said client, and the demand from the browser to display is received. An authentication means to attest the user using said browser from the individual humanity news memorized by the individual humanity news storage means, and to accumulate the information about authentication in an authentication condition storage means, The issuance domain information that the Internet domain name which publishes Cookie for writing information in a browser memorized by the issuance domain storage means is expressed is acquired. An issuance domain acquisition means to generate the domain information showing the domain attribute of said Cookie, A Cookie issuance page sending-out means to transmit the Cookie issuance page for writing in said Cookie to said browser, While making it function as a Cookie issuance means which writes in said Cookie to said browser to the demand from said browser It processes in harmony with the name resolution server program operated as a name resolution server which uses a domain name solution means for a computer, and is changed into the communication link address from the Internet domain name. The Internet domain name from which plurality differs is related with the communication link address of said one authentication server, and the authentication server program characterized by making it function on a computer as performing authentication processing in common is acquired from said two or more service servers.
[0023] According to this invention, it sets to said authentication server program. Moreover, said authentication means Identification information, such as a user's ID and a password, from said browser Reception, If the authentication information about a user will newly be created and it will accumulate in said authentication condition storage means as compared with said identification information accumulated in said individual humanity news storage means, if a match is in said individual humanity news storage means, and there is no match While having the function which notifies authentication failure to said browser, said service server program The Cookie published with said Cookie issuance means is read, and the authentication server program characterized by being a program for operating as a computer whether the user using said browser is attested as a Cookie acquisition means to judge is acquired.
[0024] Moreover, according to this invention, in said authentication server program, said issuance domain acquisition means acquires said issuance domain information from said issuance domain storage means, and the authentication server program characterized by generating the domain information which deleted the character string showing said authentication server from said issuance domain information is acquired.
[0025] According to this invention, it sets to said authentication server program. Moreover, said Cookie issuance page sending-out means It acquires with said authentication information generated with said authentication

means, and said issuance domain acquisition means. Said Cookie issuance page which performs the communication link to said Cookie issuance means which writes in said Cookie to said browser from said generated issuance domain information and said domain information is generated, and the authentication server program characterized by answering a browser is acquired.

[0026] Moreover, according to this invention, in said authentication server program, said Cookie issuance means generates said Cookie from said authentication information described in said Cookie issuance page received by said browser, and said domain information, and the authentication server program characterized by writing the Cookie concerned in a communication link demand from said browser at said browser is acquired.

[0027] According to this invention, it sets to said authentication server program. Moreover, said Cookie acquisition means In said service server which provides a user with various services, it functions on the Internet. Said Cookie issuance means by reading said Cookie written in said browser, and comparing said authentication information described in the Cookie concerned with said authentication information accumulated in said authentication condition storage means It has the function to judge whether said browser is already attested, and the authentication server program characterized by cooperating with said service server is acquired.

[0028]

[Embodiment of the Invention] Hereafter, it explains, referring to a drawing about the gestalt of operation of this invention.

[0029] Drawing 1 is drawing showing the configuration of the information processing system by the gestalt of operation of this invention.

[0030] It has the name resolution server 2 for changing into the actual communication link address, two or more service servers 3 to which the World-Wide-Web server (WWW server) for providing a user with service through the Internet actually is operating, and the authentication server 4 which attests by performing log in processing of a user from many and unspecified clients 1 which a general user uses in information processing system 10 as shown in drawing 1 , and the identifier on the Internet, and is constituted. Here, the client 1, the name resolution server 2, the service server 3, and the authentication server 4 are connected through networks, such as the Internet. A name resolution server program, a service server program, and the authentication server program 4 can be made to perform each function of the name resolution server 2, the service server 3, and an authentication server 4 to a computer, respectively.

[0031] On a client 1, the browser 11 is operating, it communicates with the name resolution server 2, the service server 3, and an authentication server 4, and the resource on a server is acquired.

[0032] Moreover, the domain name solution means 12 is operating on the name resolution server 2, and transform processing from the host name which showed the host on the Internet based on the information memorized by the domain information storage means 151 to the actual communication link address is performed. Generally the domain name solution means 12 is called a domain name server (DNS), and is specified to No. 1034 of RFC which described the criterion of the Internet, and No. 1035.

[0033] A table 1 shows the example of a content of the domain information record means 5.

[0034]

[A table 1]

インターネット上のホスト名	通信アドレス
www.jr-odekake.net	123.4.5.6
www.jrwest.co.jp	10.5.6.7

[0035] The example shown in a table 1 shows that the host name "www.jr-odekake.net" is changed into the communication link address "123.4.5.6", and the host name "www.jrwest.co.jp" is changed into the communication link address "10.5.6.7."

[0036] The domain name solution means 12 may be operating in cooperation on two or more name resolution servers 2, and may also have two or more domain information storage means 5.

[0037] The WWW server is operating to the service server 3, and a letter is answered [communication link / using HTTP from a browser 11] in reception and a resource. This WWW server has the expanded capability of a server, and the Cookie acquisition means 13 for acquiring the authentication information accumulated in the browser 11 as Cookie using the device concerned is operating.

[0038] Moreover, the WWW server which is the same as the service server 3, or has this function also on an authentication server 4 is operating, and reception and log in processing are performed for the communication link using HTTP from a browser 11. This WWW server has the expanded capability of a server. The device is used. The log in demand from a browser 11 It receives. Actual log in processing When the authentication means 14 and log in to perform are successful, Cookie The domain information to publish A browser 11 is received

actually. the Cookie issuance page sending-out means 16 for sending out the Cookie issuance page for writing in Cookie to a browser 11 based on the domain information acquired with the issuance domain acquisition means 15 and the issuance domain acquisition means 15 of acquiring -- The Cookie issuance means 17 for publishing Cookie is operating. Moreover, the issuance domain storage means 8 for accumulating the host name of the authentication server 4 which publishes the authentication condition storage means 7 and Cookie for accumulating the authentication condition of the individual humanity news storage means 6 for accumulating the individual humanity news of the user using a browser 11 and a browser 11 is connected to the service server 3 and the authentication server 4.

[0039] The individual humanity news storage means 6, the authentication condition storage means 7, and the issuance domain storage means 8 may be mounted in a world wide web server in order to mitigate the time and effort of a system construction.

[0040] As an example of the gestalt of operation of this invention, three service servers 3 exist and suppose that the host name had the identifier of "www.jr-odekake.net", "www.nec.co.jp", and "ecsite.jrwest.co.jp." At this time, domain information on each service server 3 is set to "jr-odekake.net", "nec.co.jp", and "jrwest.co.jp."

[0041] The authentication server 4 in the gestalt of operation of this invention adds the character string which shows that it is an authentication server 4 to the domain information for each servers, and has two or more host names in it. For example, when the character string which shows that it is an authentication server 4 is set to "ninsyou", it has three identifiers, "ninsyou.jr-odekake.net", "ninsyou.nec.co.jp", and "ninsyou.jrwest.co.jp." Only the number of the classes of domain information on the service server 3 that the host name which an authentication server 4 has here attests in common has a host name. When two or more of a certain service servers 3 have the same domain information, an authentication server 4 should just have one host name to the domain information.

[0042] The following table 2 shows the example of the domain information storage means at this time.

[0043]

[A table 2]

インターネット上のホスト名	通信アドレス
www.jr-odekake.net	123.4.5.6
ninsyou.jr-odekake.net	123.4.5.100
www.nec.co.jp	192.168.1.10
ninsyou.nec.co.jp	123.4.5.100
ecsite.jrwest.co.jp	10.5.6.8
ninsyou.jrwest.co.jp	123.4.5.100

[0044] As shown in the above-mentioned table 2, each service server is registered as "www.jr-odekake.net", "www.nec.co.jp", and "ecsite.jrwest.co.jp", and each communication link address is set up with "123.4.5.6", "192.168.1.10", and "10.5.6.8." Moreover, the host name corresponding to each service server 3 of an authentication server 4 is registered as "ninsyou.jr-odekake.net", "ninsyou.nec.co.jp", and "ninsyou.jrwest.co.jp", and since each host name points out the same authentication server 4, the communication link address becomes the same thing. When the communication link addresses which show the authentication server 4 memorized by the domain information storage means 5 here differ, you may make it the same communication link address eventually shown using a device with the conversion function of the communication link address which controls a communicative path and which is generally called a router and a switch. Moreover, when an authentication server 4 equips two or more communication equipment and can use two or more communication link addresses, the communication link address which shows the authentication server 4 memorized with the domain information storage means 5 may be shown by two or more communication link addresses.

[0045] A table 3 shows the domain information which the issuance domain storage means 8 at this time has.

[0046]

[A table 3]

発行ドメイン情報
ninsyou.jr-odekake.net
ninsyou.nec.co.jp
ninsyou.jrwest.co.jp

[0047] Drawing 2 is flow chart drawing showing the actuation about log in processing of a user.
[0048] Log in processing of a user is explained based on the above example, referring to drawing 2 .
[0049] First, an authentication server 4 receives ID and password of the user who uses the browser 11 with the authentication means 14 on a WWW server from a browser 11 (step S1). If it is the information which can specify users, such as fingerprint information, at this time, you may use as a substitute of ID and a password. The authentication means 14 which received ID and a password compares ID and the password which were received from ID and the password which are accumulated in the individual humanity news storage means 6, and the browser 11 (step S2).
[0050] A table 4 shows an example of the individual humanity news storage means 6 at this time.
[0051]
[A table 4]

ID	パスワード
XYZ00001	QLsiJD11
...	...

[0052] As shown in the above-mentioned table 4, this example shows that the password of the user of ID "XYZ00001" is "QLsiJD11." With the individual humanity news storage means 6, the information on the name about a user, an address, etc. may be collectively memorized besides said ID and password. Moreover, the information on ID, a password, etc. may be enciphered by a certain code approach. Next, as a result of the comparison of ID and a password, it checks whether it is in agreement (step S3), and when not in agreement, authentication failure is notified to a browser 11 and log in (step S4) processing is ended. When in agreement, the authentication information which shows that a browser 11 is authentication ending is generated (step S5). As long as this authentication information serves as a peculiar value every browser 11, what kind of value is sufficient as it. The generated authentication information is accumulated in the authentication condition storage means 7 with ID (step S6).
[0053] A table 5 shows an example of the authentication condition storage means 7 at this time.
[0054]
[A table 5]

ID	認証情報
XYZ00001	IOJ99312-3333jd
...	...

[0055] The example shown in a table 5 shows that ID "XYZ00001" is attested for authentication information "IOJ99312-3333jd." At this time, with the authentication information storage means 7, the time amount at the time of a log in success etc. may be accumulated other than said ID and authentication information, and you may use for time-out processing etc. Next, the issuance domain acquisition means 15 acquires the issuance domain information on Cookie from the issuance domain storage means 8 (step S7).
[0056] "ninsyou.jr-odekake.net", "ninsyou.nec.co.jp", and "ninsyou.jrwest.co.jp" are acquired in the example of a table 3. The issuance domain acquisition means 15 creates the domain information which deleted the character string which shows an authentication server 4 from the acquired issuance domain information (step S8). "jr-odekake.net", "nec.co.jp", and "jrwest.co.jp" are created in the aforementioned example. Next, the Cookie issuance page sending-out means 16 creates a Cookie issuance page based on the authentication information generated and acquired at steps S5, S7, and S8, issuance domain information, and domain information, and answers a browser 11 (step S9).
[0057] Drawing 3 is drawing showing the example of the Cookie issuance page in said example. To be shown in drawing 3 , this Cookie issuance page is described with the description language generally called HTML, and can order various processings to a browser 11 by being interpreted by the browser 11. It is detailed to "HyperText Markup Language Home Page" acquirable by URL of "http://www.w3c.org/MarkUp/" about HTML.
[0058] the description about the Cookie issuance among the HTML description shown by drawing 3 — <FRAME .... it is the line shown by >. <FRAME ... > orders a browser 111 to access URL shown according to the item of solvent refined coal. For example, <FRAME solvent-refined-coal="http://ninsyou.jr-odekake.net/cookie?C_ID=IOJ99312-3333 jd&DOM_NAME=jr-odekake.net" > As opposed to the Cookie issuance means 17 specified by the identifier of cookie from the authentication server 4 shown by ninsyou.jr-odekake.net It was specified as the argument by having made domain information on Cookie "jr-odekake.net" into DOM_NAME, having used

authentication information "IOJ99312-3333jd" as C_ID, and the browser 11 is ordered to access. At this time, a browser 11 is <FRAME. ... [... > description may be used.] It has, when > description cannot be processed, and <NOFRAMES> description is used, and it is <FRAME... It is <IMAGE instead of > description. Moreover, <FRAME described to a Cookie issuance page ... > is set only to one, performs description which calls the Cookie issuance means 17 accessed by other host names during the reply of the Cookie issuance means 17, and may be made to publish Cookie one by one. The browser 11 which received the Cookie issuance page accesses the Cookie issuance means 17 on an authentication server 4 according to the HTML description in a page (step S10). The Cookie issuance means 17 creates Cookie information by making into a domain attribute domain information which specified the authentication information described as C_ID as a value of Cookie, and was specified as DOM_NAME in URL at the time of access, and writes it in using the Set-Cookie header of HTTP described above to the browser 11 (step S11). For example the Cookie issuance means 17 — <FRAME When called by HTML description of solvent-refined-coal="http://ninsyou.jr-odekake.net/cookie?C_ID=IOJ99312-3333jd&DOM_NAME=jr-odekake.net" >, "IOJ99312-3333jd" and domain information serve as [authentication information] "jr-odekake.net". The Cookie issuance means 17 "Set-Cookie : C_ID=IOJ99312-3333jd The header; domain=jr-odekake.net" is transmitted to a browser 11. As the browser 11 which received this header was described above, the Cookie issuance means 17 is referred to by the host name of "http://ninsyou.jr-odekake.net", since the domain attribute "jr-odekake.net" specified as Cookie is included, the writing of Cookie is permitted, and a value saves [an identifier] the Cookie of "IOJ99312-3333jd" by "C_ID." Only the part of the <FRAME> description the browser 11 is described to be in the Cookie issuance page repeats step S10 and step S11.

[0059] In the example, although the Cookie issuance means 17 on ninsyou.jr-odekake.net, ninsyou.nec.co.jp, and ninsyou.jrwest.co.jp will be referred to, this shows the communication link address to the same authentication server 4 altogether as it is shown in a table 2.

[0060] On the browser 11 which succeeded in the log in, the Cookie for each service server 3 on a local area network is written in by the above step of S1-S11.

[0061] Next, drawing 4 is drawing with which explanation of the service server's 3 which offers the service for specific users authentication processing of access from a browser 11 of a carrier beam case is presented. If drawing 4 is referred to, when the service server 3 has access from a browser 11, a browser 11 will investigate first whether authentication information is transmitted as Cookie (step S21). If the step of steps S1-S11 which the browser 11 mentioned above is performing log in processing at this time, as described above, a browser 11 will add a Cookie header during the HTTP communication link to an authentication server 4, and will transmit the authentication information memorized as Cookie by this Cookie header to an authentication server 4.

[0062] If the browser 11 has not transmitted authentication information as Cookie, by the authentication server 4, authentication information is unreceivable, and the browser 11 refuses the service for specific users noting that it is not attested (step S22). If authentication information is receivable as Cookie by the authentication server 4, it will investigate whether the authentication information concerned is accumulated with the authentication condition storage means 7 (steps S23 and S24). At this time, in order to raise safety, processing whose authentication information concerned checks whether it is the right using a code technique etc. may be performed. If the received authentication information is not accumulated with the authentication storage means 7, the service for specific users is refused noting that it is unjust authentication information (S25). If the received authentication information is accumulated in the authentication storage means 7, the accessed browser 11 will presuppose that it is already authentication ending, and will permit utilization of the service for specific users to a browser 11. By each step of steps S21-S26, the browser 11 which each service server 3 has accessed can distinguish whether it is authentication ending. In addition, when the service for specific users is refused in each step of steps S22 and S25, a transfer etc. may be processed and the log in processing by the authentication server 4 may be demanded from a user.

[0063] As mentioned above, in order to raise safety to the communication link between step S1 - the client 1 in each step of S11, S21-S26 and the service server 3 and an authentication server 4, it is desirable to encipher the content of a communication link. Make it moreover, more desirable to operate on the same local area network in the service server 3, an authentication server 4, the individual humanity news storage means 6, the authentication condition storage means 7, and the issuance domain storage means 8 in order to raise safety. Moreover, it is more desirable to use the communication device with a browser 11 generally known as a fire wall in the case of a communication link, and to raise communicative safety.

[0064]

[Effect of the Invention] As explained above, the user who uses the browser by using this invention Since authentication information will be shared by two or more service servers from which a domain differs once it merely logs in, The time and effort which redoes a log in for every server is lost, and it becomes easy for this to

uide the user using a certain service server to the service server which is operating on other domains. The ıformation processing system to which the number of users using service can be made to increase can be ffered.

)065] Moreover, in this invention, the Internet domain name to which the user who could give his name and was ased on the content of service tends to memorize what kind of Internet domain name in case each service erver is built can be used, this becomes possible to impress the Internet domain name of a service server eeply to many and unspecified users, and the information processing system to which the number of users sing service can be made to increase can be offered.

Translation done.]

: NOTICES *

PO and NCIPI are not responsible for any
lamages caused by the use of this translation.

.This document has been translated by computer. So the translation may not reflect the original precisely.
!.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

)ESCRIPTION OF DRAWINGS

Brief Description of the Drawings]
Drawing 1] It is the block diagram showing the information processing system by the gestalt of operation of this nvention.
Drawing 2] It is flow chart drawing with which explanation of the information processing system of drawing 1 of operation is presented.
Drawing 3] It is drawing showing an example of the Cookie issuance page published by the information processing system of the gestalt of operation of this invention.
[Drawing 4] It is flow chart drawing showing judgment processing of the attested browser in the service server of the information processing system by the gestalt of operation of this invention.
[Description of Notations]
1 Client
2 Name Resolution Server
3 Service Server
4 Authentication Server
5 Domain Information Storage Means
6 Individual Humanity News Storage Means
7 Authentication Condition Storage Means
8 Issuance Domain Storage Means
10 Information Processing System
11 Browser
12 Domain Name Solution Means
13 Cookie Acquisition Means
14 Authentication Means
15 Issuance Domain Acquisition Means
16 Cookie Issuance Page Sending-Out Means
17 Cookie Issuance Means

[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any
damages caused by the use of this translation.